



500.41092X00

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicants: M. NISHIOKA et al.

Serial No.: 10/046,224

Filed: January 16, 2002

For: PUBLIC-KEY CRYPTOGRAPHIC SCHEMES SECURE  
AGAINST AN ADAPTIVE CHOSEN CIPHER TEXT ATTACK IN  
THE STANDARD MODEL

Group: 2136

Examiner: D. G. Cervetti

**INFORMATION DISCLOSURE STATEMENT  
UNDER 37 CFR §1.97 & 1.98**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

In the matter of the above-identified application, Applicants are submitting herewith a form equivalent to Form PTO-1449 for the Examiner's consideration.

In response to the Office Action dated February 7, 2006, Applicants submit herewith a copy of the document "Non-Malleable Cryptography" as requested by the Examiner.

In response to the Advisory Action dated September 21, 2006, Applicants submit herewith a copy of the "Random Oracle" as requested by the Examiner.

This Information Disclosure Statement is being submitted after a first Office Action has been received and is accompanied by the required fee in the amount of \$180.00

02/12/2007 #ABDELRI 00000037 10046224


02 FC:1806 180.00 0P

It is respectfully requested that this information disclosure statement be considered by the Examiner.

Please charge any shortage in the fees due in connection with the filing of this paper, including extension of time fees, to the deposit account of Mattingly, Stanger, Malur & Brundidge, Deposit Account No. 50-1417 (referencing attorney docket no. 500.41092X00) please credit any excess fees to such deposit account.

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.



---

Carl I. Brundidge  
Registration No. 29,621

CIB/DKM/cmd  
(703) 684-1120

**FORM PTO-1449** U.S. Department of  
Commerce (Rev. 4/92) Patent and Trademark

ATTY. DOCKET NO.

SERIAL NO.

500.41092X00

10/046,224

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**

(Use several sheets if necessary)

APPLICANT  
M. NISHIOKA et al.

FILING DATE  
January 16, 2002

GROUP  
2136

**U.S. PATENT DOCUMENTS**

| EXAMINER<br>INITIAL | DOCUMENT NUMBER | DATE | NAME | CLASS | SUBCLASS | FILING DATE<br>IF APPROPRIATE |
|---------------------|-----------------|------|------|-------|----------|-------------------------------|
|                     |                 |      |      |       |          |                               |
|                     |                 |      |      |       |          |                               |
|                     |                 |      |      |       |          |                               |
|                     |                 |      |      |       |          |                               |
|                     |                 |      |      |       |          |                               |
|                     |                 |      |      |       |          |                               |
|                     |                 |      |      |       |          |                               |
|                     |                 |      |      |       |          |                               |
|                     |                 |      |      |       |          |                               |

**FOREIGN PATENT DOCUMENTS**

|  | DOCUMENT NUMBER | DATE | COUNTRY | CLASS | SUBCLASS | ABSTRACT |    |
|--|-----------------|------|---------|-------|----------|----------|----|
|  |                 |      |         |       |          | YES      | NO |
|  |                 |      |         |       |          |          |    |
|  |                 |      |         |       |          |          |    |
|  |                 |      |         |       |          |          |    |
|  |                 |      |         |       |          |          |    |
|  |                 |      |         |       |          |          |    |

**OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)**

|  |   |
|--|---|
|  | D. Dolev, et al "Non-Malleable Cryptography", In 23 <sup>rd</sup> Annual ACM Symposium on Theory of Computing, pp. 542-552, 1991. |
|  | R. Cramer, et al. "A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack", pp. 1-18.      |
|  | "Random Oracle". ( <a href="http://en.wikipedia.org/wiki/Random_Oracle">http://en.wikipedia.org/wiki/Random_Oracle</a> )          |

EXAMINER

DATE CONSIDERED

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.